CLAIMS

1. An information recorder to record information to a recording medium, the apparatus comprising:

a cryptography means having a node key unique to each of nodes included in a hierarchical tree structure in which a plurality of different information recorders is included as each of leaves of the tree structure and a leaf key unique to each of the information recorders, and which encrypts data to be stored into the recording medium;

the cryptography means generating an encryption key based on encryption key generating data built in the information recorder to encrypt data to be stored into the recording medium; and

the encryption key generating data being data which can be renewed with at least either the node key or leaf key.

2. The apparatus according to claim 1, wherein the encryption key generating data is a master key common to the plurality of information recorders.

3. The apparatus according to claim 1, wherein the encryption key generating data is a medium key unique to a specific recording medium.

4. The apparatus according to claim 1, wherein:

the node key can be renewed;

there is distributed, when a node key is renewed, a key renewal block (KRB) derived from encryption of the renewal node key with at least either a node key or leaf key on a lower stage of the tree structure to an information recorder at a leaf where the encryption key generating data has to be renewed; and

the cryptography means in the information recorder receives a renewal data for the encryption key generating data encrypted with the renewed node key, encrypts the key renewal block (KRB) to acquire the renewed node key, and calculates a renewal data for the encryption key generating data based on the renewed node key thus acquired.

5. The apparatus according to claim 4, wherein:

the key renewal block (KRB) is stored in a recording medium; and

the cryptography means encrypts the key renewal block (KRB) read from the recording medium.

6. The apparatus according to claim 1, wherein:

the encryption key generating data has a generation number as renewal information correlated therewith; and

the cryptography means stores, as a recording generation number into the recording member, a generation number of the encryption key generating data having been used when storing encrypted data into the recording medium.

7. The apparatus according to claim 1, wherein the following encrypting procedures are selectively effected depending upon whether a player restriction is set or not:

when the player restriction is not set, a first encryption key is generated for data to be stored into the recording medium based on a first encryption key generating data to encrypt the data to be stored into the recording medium with the first encryption key and the first encryption key generating data is stored into the recording medium; and

when the player restriction is set, a second encryption key for the data to be stored into the recording medium is generated based on a second encryption key generating data built in the information recorder to encrypt the data to be stored into the recording medium with the second encryption key.

8. The apparatus according to claim 7, wherein the cryptography means does as follows depending upon whether the player restriction is set or not:

when the player restriction is not set, the cryptography means generates a title-unique key from a master key, of which the generation is managed, stored in the information recorder, a disc ID being an identifier unique to a recording medium, a title key unique to data to be recorded to the recording medium and a device ID being an identifier for the information recorder to generate the first encryption key from the title-unique key; and

when the player restriction is set, the cryptography means generates a title-unique key from the generation-managed master key stored in the information recorder, disc ID being an identifier unique to the recording medium, title key unique to the data to be recorded to the recording medium and the device-unique key unique to the information recorder to generate the second encryption key from the title-unique key.

9. The apparatus according to claim 1, further comprising a transport stream processing means for appending an arrival time stamp (ATS) to each of discrete transport packets included in a transport stream;

the cryptography means generating a block key as an encryption key for a block data including more than one packet each having the arrival time stamp (ATS) appended thereto; and

the cryptography means generating a block key as an encryption key, in encryption of the data to be stored into the recording medium, based on data including the encryption key generating data and a block seed being additional information unique to the block data including the arrival time stamp (ATS).

10. The apparatus according to claim 1, wherein the cryptography means encrypts the data to be stored into the recording medium according to DES algorithm.

11. The apparatus according to claim 1, wherein:

there is provided an interface means for receiving information to be recorded to a recording medium;

the interface means identifying copy control information appended to each of packets included in a transport stream in a data to judge, based on the copy control information, whether or not recording to the recording medium is possible.

12. The apparatus according to claim 1, wherein:

there is provided an interface means for receiving information to be recorded to a recording medium;

the interface means identifying 2-bit EMI (encryption mode indicator) as copy control information to judge, based on the EMI, whether or not recording to the recording medium is possible.

13. An information player to play back information from a recording medium, the apparatus holding a node key unique to each of nodes included in a hierarchical tree structure in which a plurality of different information recorders is included as each of leaves of the tree structure and a leaf key unique to each of the information recorders, comprising a cryptography means to decrypt encrypted data stored in the recording medium;

the cryptography means generating a decryption key based on decryption key generating data built in the information recorder to decrypt the encrypted data stored in the recording medium; and

the decryption key generating data being data which can be renewed with at least either the node key or leaf key.

14. The apparatus according to claim 13, wherein the decryption key generating data is a master key common to the plurality of information recorders.

15. The apparatus according to claim 13, wherein the decryption key generating data is a medium key unique to a specific recording medium.

16. The apparatus according to claim 13, wherein:

the node key can be renewed;

there is distributed, when a node key is renewed, a key renewal block (KRB) derived from encryption of the renewal node key with at least either a node key or leaf key on a lower stage of the tree structure to an information player at a leaf where the encryption key generating data has to be renewed; and

the cryptography means in the information recorder receives a renewal data for the decryption key generating data encrypted with the renewed node key, encrypts the key renewal block (KRB) to acquire the renewed node key, and calculates a renewal data for the decryption key generating data based on the renewed node key thus acquired.

17. The apparatus according to claim 16, wherein:

the key renewal block (KRB) is stored in a recording medium; and

the cryptography means encrypts the key renewal block (KRB) read from the recording medium.

18. The apparatus according to claim 13, wherein:

the decryption key generating data has a generation number as renewal information correlated therewith; and

the cryptography means reads, from the recording medium when decrypting encrypted data read from the recording medium, a generation number of the encryption key generating data having been used when encrypting the encrypted data and generates a decryption key from the decryption key generating data corresponding to the generation number thus read.

19. The apparatus according to claim 13, wherein the following decrypting procedures are selectively effected depending upon a player restriction is set or not:

when the player restriction is not set, a first decryption key is generated for the encrypted data stored in the recording medium based on a first decryption key generating data stored in the recording medium to decrypt the encrypted data with the first decryption key; and

when the player restriction is set, a second decryption key for the encrypted data stored in the recording medium is generated based on a second encryption key generating data built in the information recorder to decrypt the encrypted data with the second decryption key.

20. The apparatus according to claim 19, wherein the cryptography means does as follows depending upon whether the player restriction is set or not:

when the player restriction is not set, the cryptography means acquires a generation-managed master key stored in the information recorder and acquires, from a recording medium, a disc ID being an identifier unique to a recording medium, a title key unique to data to be decrypted and a device ID being an identifier for the information recorder having recorded the encrypted data to generate a title-unique key from the master key, disc ID, title key and device key and the first decryption key from the title-unique key; and

when the player restriction is set, the cryptography means acquires a generation-managed master key stored in the information recorder and a device-unique key unique to, and stored in, the information recorder and acquires, from a recording medium, a disc ID being an identifier unique to the recording medium and a title key unique to the data to be decrypted to generate a title-unique key from the master key, disc ID, title key and device-unique key, and the second decryption key is generated from the title-unique key.

21. The apparatus according to claim 13, further comprising a transport stream processing means for controlling data outputting based on an arrival time stamp (ATS) appended to each of a plurality of transport packets included in the block data having been decrypted by the cryptography means;

the cryptography means generating a block key as a decryption key for a block data including more than one packets each having the arrival time stamp (ATS) appended thereto; and

the block key as a decryption being generated, in decryption of the encrypted data stored in the recording medium, based on data including the decryption key generating data and a block seed being additional information unique to the block data including the arrival time stamp (ATS).

22. The apparatus according to claim 13, wherein the cryptography means decrypts the encrypted data stored in the recording medium according to DES algorithm.

23. The apparatus according to claim 13, wherein there is further provided an interface means for receiving information to be recorded to a recording medium;

the interface means identifying copy control information appended to each of packets included in a transport stream in a data to judge, based on the copy control information, whether or not playback from the recording medium is possible.

24. The apparatus according to claim 13, wherein there is further provided an interface means for receiving information to be recorded to a recording medium;

the interface means identifying 2-bit EMI (encryption mode indicator) as copy control information to judge, based on the EMI, whether or not playback from the recording medium is possible.

25. An information recording method for recording information to a recording medium, the method comprising the steps of:

renewing encryption key generating data to generate an encryption key for encrypting data to be stored into a recording medium with at least either a node key unique to each of nodes included in a hierarchical tree structure in which a plurality of different information recorders is included as each of leaves of the tree structure or a leaf key unique to each of the information recorders; and

generating an encryption key based on the encryption key generating data to encrypt data to be stored into the recording medium.

26. The method according to claim 25, wherein the encryption key generating data is a master key common to the plurality of information recorders.

27. The method according to claim 25, wherein the encryption key generating data is a medium key unique to a specific recording medium.

28. The method according to claim 15, wherein:

the node key can be renewed;

there is distributed, when a node key is renewed, a key renewal block (KRB) derived from encryption of the renewal node key with at least either a node key or leaf key on a lower stage of the tree structure to an information recorder at a leaf where the encryption key generating data has to be renewed; and

the renewing step comprises steps of:

acquiring the renewed node key by encrypting the key renewal block (KRB); and

calculating a renewal data for the encryption key generating data based on the renewed node key thus acquired.

29. The method according to claim 25, wherein:

the encryption key generating data has a generation number as renewal information correlated therewith; and

the cryptography step further includes the step of storing, when storing encrypted data into the recording medium, a generation number of the encryption key generating data having been used, as a recording generation number into the recording medium.

30. The method according to claim 25, wherein the cryptography step includes the following two procedures, either of which is to selectively be effected depending upon whether a player restriction is set or not:

when the player restriction is not set, a first encryption key is generated for data to be stored into the recording medium based on a first encryption key generating data, the data to be stored into the recording medium is encrypted with the first encryption key and the first encryption key generating data is stored into the recording medium; and

when the player restriction is set, a second encryption key for the data to be stored into the recording medium is generated based on a second encryption key generating data built in the information recorder and the data to be stored into the recording medium is encrypted with the second encryption key.

31. The method according to claim 30, wherein the cryptography means does as follows depending upon whether the player restriction is set or not:

when the player restriction is not set, the cryptography means generates a title-unique key from a generation-managed master key stored in the information recorder, a disc ID being an identifier unique to a recording medium, a title key unique to data to be recorded to the recording medium and a device ID being an identifier for the information recorder and generates the first encryption key from the title-unique key; and

when the player restriction is set, the cryptography means generates a title-unique key from the generation-managed master key stored in the information recorder, disc ID being an identifier unique to the recording medium, title key unique to the data to be recorded to the recording medium and the device-unique key unique to the information recorder and generates the second encryption key from the title-unique key.

32. The method according to claim 25, wherein there is further included a transport stream processing step of appending an arrival time stamp (ATS) to each of discrete transport packets included in a transport stream; in the cryptography step:

there is generated a block key as an encryption key for a block data including more than one packet each having the arrival time stamp (ATS) appended thereto; and

the block key as an encryption key is generated, in encryption of the data to be stored into the recording medium, based on data including the encryption key generating data and a block seed being additional information unique to the block data including the arrival time stamp (ATS).

33. The method according to claim 25, wherein there is encrypted in the cryptography step the data to be stored into the recording medium according to DES algorithm.

34. The method according to claim 25, wherein copy control information appended to each of packets included in a transport stream in a data is identified to judge, based on the copy control information, whether or not recording to the recording medium is possible.

35. The method according to claim 25, wherein 2-bit EMI (encryption mode indicator) as copy control information is identified to judge, based on the EMI, whether or not recording to the recording medium is possible.

36. An information playback method to play back information from a recording medium, the method comprising the steps of:

renewing decryption key generating data from which there is generated a decryption key for decryption of encrypted data stored in the recording medium with at least either a node key unique to each of nodes included in a hierarchical tree structure in which a plurality of different information players is included as each of leaves of the tree structure or a leaf key unique to each of the information players; and

generating the decryption key from the decryption key generating data having renewed in the renewing step to decrypt the data stored in the recording medium.

37. The method according to claim 36, wherein the decryption key generating data is a master key common to the plurality of information recorders.

38. The method according to claim 36, wherein the decryption key generating data is a medium key unique to a specific recording medium.

39. The method according to claim 36, wherein:

the node key can be renewed;

there is distributed, when a node key is renewed, a key renewal block (KRB) derived from encryption of the renewal node key with at least either a node key or leaf key on a lower stage of the tree structure to an information player at a leaf where the encryption key generating data has to be renewed; and

the cryptography step comprises the steps of:

encrypting the key renewal block (KRB) to acquire the renewed node key; and calculating a renewal data for the decryption key generating data based on the renewed node key thus acquired.

40. The method according to claim 36, wherein:

the decryption key generating data has a generation number as renewal information correlated therewith; and

in the cryptography step, there is read from the recording medium when decrypting encrypted data from the recording medium, a generation number of the encryption key generating data having been used when encrypting the encrypted data to generate a decryption key from decryption key generating data corresponding to the generation number thus read.

41. The method according to claim 36, wherein the cryptography step includes the following two procedures, either of which is to selectively be effected depending upon whether a player restriction is set or not:

when the player restriction is not set, a first decryption key is generated for encrypted data stored in the recording medium based on a first decryption key generating data stored in the recording medium, the encrypted data is decrypted with the first decryption key; and

when the player restriction is set, a second decryption key for the encrypted data stored in the recording medium is generated based on a second encryption key generating data built in the information recorder and the encrypted data is decrypted with the second decryption key.

42. The method according to claim 41, wherein the cryptography step includes the following two procedures:

when the player restriction is not set, there is acquired a generation-managed master key stored in the information recorder and also acquired, from a recording medium, a disc ID being an identifier unique to a recording medium, a title key unique to data to be decrypted and a device ID being an identifier for the information recorder having recorded the encrypted data to generate a title-unique key from the master key, disc ID, title key and device key and the first decryption key from the title-unique key; and

when the player restriction is set, there is acquired a generation-managed master key stored in the information recorder and a device-unique key unique to, and stored in, the information recorder and also acquired, from a recording medium, a disc ID being an identifier unique to the recording medium and a title key unique to the data to be decrypted to generate a title-unique key from the master key, disc ID, title key and device-unique key; and the second decryption key being generated from the title-unique key thus generated.

43. Th method according to claim 36, wherein:

the player includes a transport stream processing means for controlling data outputting based on an arrival time stamp (ATS) appended to each of a plurality of transport packets included in the decrypted block; and in the cryptography step:

a block key is generated as a decryption key for a block data including more than one packets each having the arrival time stamp (ATS) appended thereto; and

the block key as a decryption is generated, in decryption of the encrypted data stored in the recording medium, based on data including the decryption key generating data and a block seed being additional information unique to the block data including the arrival time stamp (ATS).

44. The method according to claim 36, wherein the encrypted data stored in the recording medium is decrypted according to DES algorithm.

45. The method according to claim 36, wherein copy control information appended to each of packets included in a transport stream in a data is identified to judge, based on the copy control information, whether or not playback from the recording medium is possible.

46. The method according to claim 36, wherein 2-bit EMI (encryption mode indicator) as copy control information is identified to judge, based on the EMI, whether or not playback from the recording medium is possible.

47. An information recording medium capable of recording information, having stored therein a key renewal block (KRB) derived from encryption of a renewed node key with at least either a node key unique to each of nodes included in a hierarchical tree structure in which a plurality of different information recorders is included as each of leaves of the tree structure and a leaf key unique to each of the information recorders.

48. The medium according to claim 47, wherein there is included data derived

from encryption, with the renewed node key, of encryption key generating data used to generate an encryption key to encrypt data to be stored into the recording medium in the information recorder.

49. The medium according to claim 47, wherein there is included data derived from decryption, with the renewed node key, of decryption key generating data used to generate a decryption key to decrypt encrypted data stored in the recording medium in the information player.

50. The medium according to claim 47, wherein there is stored generation information on the encryption or decryption key generating data.

51. A recording medium producing apparatus for producing an information recording medium, the apparatus comprising:

a memory to store a key renewal block (KRB) derived from encryption of a renewed node key with at least either a node key unique to each of nodes included in a hierarchical tree structure in which a plurality of different information recorders is included as each of leaves of the tree structure and a leaf key unique to each of the information recorders; and

a control unit to control write of the key renewal block (KRB) stored in the memory to the recording medium.

52. The apparatus according to claim 51, wherein:

the memory further stores at least any of a recording medium identifier and encrypted encryption key generating data or encrypted decryption key generating data;

and

the control unit controls write, to the recording medium, of at least any of the recording medium identifier and encrypted encryption key generating data or encrypted decryption key generating data.

53. The apparatus according to claim 51, wherein:

the memory further stores generation information on the encryption key generating data or decryption key generating data; and

the control unit controls write of the generation information to the recording medium.

54. A recording medium producing method comprising the steps of:

storing, into a memory, a key renewal block (KRB) derived from encryption of a renewed node key with at least either a node key unique to each of nodes included in a hierarchical tree structure in which a plurality of different information recorders is included as each of leaves of the tree structure and a leaf key unique to each of the information recorders; and

writing, to the recording medium, the key renewal block (KRB) stored in the memory.

55. The method according to claim 54, wherein:

there is further stored into the memory at least any of a recording medium identifier and encrypted encryption key generating data or encrypted decryption key generating data; and there is written to the recording medium at least any of the recording medium identifier and encrypted encryption key generating data or encrypted decryption key generating data.

56. The method according to claim 54, wherein:

generation information on the encryption key generating data or decryption key generating data is stored into the memory; and

write of the generation information to the recording medium is controlled.

57. A program serving medium for serving a computer program under which information processing for recording information to a recording medium is conducted in a computer system, the computer program comprising the steps of:

renewing encryption key generating data to generate an encryption key for encrypting data to be stored into a recording medium with at least either a node key unique to each of nodes included in a hierarchical tree structure in which a plurality of different information recorders is included as each of leaves of the tree structure or a leaf key unique to each of the information recorders; and

generating an encryption key based on the encryption key generating data to encrypt data to be stored into the recording medium.

58. A program serving medium for serving a computer program under which information stored in a recording medium is played back in a computer system, the computer program comprising the steps of:

renewing decryption key generating data from which there is generated a decryption key for decryption of encrypted data stored in the recording medium with at least either a node key unique to each of nodes included in a hierarchical tree structure in which a plurality of different information players is included as each of leaves of the tree structure or a leaf key unique to each of the information players; and

generating the decryption key from the decryption key generating data having renewed in the renewing step to decrypt the data stored in the recording medium.